UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 17-CR-124

v.

MARCUS HUTCHINS,

Defendant.

DEFENDANT'S MOTION TO DISMISS THE INDICTMENT (FAILURE TO STATE OFFENSES)

Defendant Marcus Hutchins seeks dismissal of all six counts of his indictment for their failure to state offenses. Fed. R. Crim. P. 12(b)(3)(A)(v).

Counts One and Six allege a conspiracy and attempt to violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A). Those counts should be dismissed because the indictment fails to allege any facts that would show Mr. Hutchins had any intent to cause "damage" to a protected computer within the meaning of the statute.

Counts Two through Five allege violations of the Wiretap Act, 18 U.S.C. §§ 2511 and 2512. Those counts fail to state an offense because software such as Kronos is not an "electronic, mechanical, or other device," as defined by the Wiretap Act.

Counts One, Five and Six should also be dismissed because the government does not allege the necessary intent and causation to state those offenses.

For all these reasons, the Court should grant this motion and dismiss the indictment against Mr. Hutchins.

***

The defense has concurrently filed two other separate motions to dismiss. The first seeks dismissal of all counts of the indictment on extraterritoriality and venue grounds. The second seeks dismissal of Counts Two and Six because they mis-describe the mental state required by the statutes at issue. This motion focuses on the indictment's failure to state offenses.

BACKGROUND

The six-count indictment centers around various alleged violations of the Computer Fraud and Abuse Act and the Wiretap Act. In Count One, Mr. Hutchins and his co-defendant are charged with conspiring to violate the CFAA. Counts Two through Four charge the defendants with advertising, sending, and selling an electronic communication interception device in violation of the Wiretap Act. Count Five charges that the defendants endeavored to intercept and procured another person to intercept electronic communications in violation

of the Wiretap Act. Finally, Count Six alleges that the defendants attempted to cause damage to a computer without authorization in violation of the CFAA.

As part of the purported conspiracy, the indictment alleges that Mr. Hutchins created the Kronos software, described as "a particular type of malware that recorded and exfiltrated user credentials and personal identifying information from protected computers." (Indictment ¶¶ 3(e), 4(a) (Dkt. No. 6).) It also alleges that Mr. Hutchins and his co-defendant later updated Kronos. (*Id.* ¶ 4(d).)

All other alleged overt acts in furtherance of the purported conspiracy pertain solely to Mr. Hutchins' co-defendant. Per the indictment, the co-defendant (1) used a video posted to YouTube to demonstrate how Kronos worked, (2) advertised Kronos on internet forums, (3) sold a version of Kronos, and (4) offered crypting services for Kronos. (*Id.* §§ 4(b), (c), (e), (f), (g).)

LEGAL STANDARD

A valid indictment "must allege that the defendant performed acts which, if proven, constituted a violation of the law that he is charged with violating." *United States v. Gimbel*, 830 F.2d 621, 624 (7th Cir. 1987). A defendant may raise the government's failure to state an offense before trial "if the basis for the motion is reasonably available and the motion can be determined without a trial on the merits." Fed. R. Crim. P. 12(b)(3)(B)(v). A court must dismiss the indictment when the allegations in the indictment fail to state an offense. *United*

States v. Risk, 843 F.2d 1059, 1060 (7th Cir. 1988). In other words, when the government's "characterization of the undisputed facts [does] not constitute a violation of any statute," there is "no case to prove." *Id*.

ARGUMENT

The indictment's six counts fail to allege acts by Mr. Hutchins which, if proven, would constitute violations of the CFAA or the Wiretap Act. Because there is "no case to prove," the Court should dismiss the indictment against Mr. Hutchins in its entirety.

1. Counts One and Six Do Not Allege Violations of the Computer Fraud and Abuse Act

Counts One and Six allege that Mr. Hutchins and his co-defendant conspired and attempted to violate 18 U.S.C. § 1030(a)(5)(A). This section prohibits "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." "Damage," in turn, is defined as "any impairment to the availability or integrity of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8).

In spite of this specific definition, the indictment claims only that Kronos "recorded and exfiltrated user credentials and personal identifying information from protected computers." (Indictment ¶¶ 4(a), 3(e).) Nothing in this description indicates that Mr. Hutchins (or his co-defendant, for that matter)

agreed or attempted to intentionally cause "impairment to the availability or integrity" of anything. They are alleged only to have "recorded and exfiltrated" data—that is, making a copy of the data and taking it away.

These actions alone do not constitute damage within the meaning of the CFAA: they do not affect the "availability" or "integrity" of the underlying data.

The Seventh Circuit has repeatedly found that "damage" requires more than what the indictment here alleges. On one end of the spectrum, in *Int'l Airport Ctrs. LLC v. Citrin*, a defendant was found to have caused damage when he installed software on his employer's computer that permanently deleted stored files. 440 F.3d 418, 419 (7th Cir. 2006). And in *United States v. Mitra*, a defendant's disruption of the functionality of Madison's emergency response system caused damage within the meaning of the CFAA. 405 F.3d 492, 494-95 (7th Cir. 2005).

On the other end of the spectrum is *Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.*, 810 F.3d 1075 (7th Cir. 2016). There, a data analytics company was accused of violating § 1030(a)(5)(A) when it used a computer program to download real estate records in bulk from county databases in violation of a technology provider's license agreement. *Id.* at 1078. The Seventh Circuit found that the company did not cause damage within the meaning of the CFAA because it did not "alter or disrupt" the technology provider's service—it

simply downloaded information while avoiding the provider's attempts to track user activity. *Id.* at 1084.

The government's allegations here are on the *Fidlar Technologies* end of the scale. Indeed, as Judge Stadtmueller has noted, "merely accessing and disseminating information" on a computer does not meet the CFAA's "very specific" definition of damage—and any claim otherwise "borders on the frivolous." *Landmark Credit Union v. Doberstein,* 746 F. Supp. 2d 990, 993-94 (E.D. Wis. 2010).

The indictment does not establish that Kronos "impaired the availability or integrity" of data, a program, a system, or information in any way. For this reason alone, the indictment fails to state an offense in Counts One and Six, and they must be dismissed.

2. Counts Two Through Five Do Not Allege Violations of the Wiretap Act

Counts Two through Four allege that Mr. Hutchins violated 18 U.S.C. § 2512 by adverting, sending, and selling an "electronic, mechanical, or other device" that is primarily useful for surreptitious interception—specifically, the Kronos software.

At 18 U.S.C. § 2510(5), the Wiretap Act specifically defines the term "electronic, mechanical, or other device" to mean "any device or apparatus which can be used to intercept a wire, oral, or electronic communication," with some exceptions not relevant in this case. While § 2510 does not specifically

define "device," undefined terms in a statute are deemed to have their ordinary meaning. *Taniguchi v. Kan Pacific Saipan, Ltd.*, 566 U.S. 560, 566 (2012).

The Merriam-Webster Dictionary defines "device" to mean, *inter alia*, "a piece of equipment or a mechanism designed to serve a special purpose or perform a special function."[1] It offers as an example of usage for this definition "a hidden recording device"—precisely the type of instrument at the heart of the Wiretap Act's prohibitions. A software program is neither a "piece of equipment" nor a "mechanism." Thus, it does not meet the ordinarily understood meaning of "device."

Turning back to the indictment, Counts Two through Four claim that Mr. Hutchins advertised, sent, and sold the Kronos software. But the three § 2512 counts cannot survive where the charges are based on advertising, sending, and selling software. Section 2512 makes it illegal only to advertise, send, or sell an "electronic, mechanical, or other device" that is primarily useful for surreptitious interception. Software is not a device because it is not an "apparatus," a "piece of equipment" or a "mechanism." It is a computer program.

The Seventh Circuit has recognized this important distinction. It held in a wiretapping case involving the use of software to intercept a communication that the computers running software were the relevant devices for purposes of the

[1] https://www.merriam-webster.com/dictionary/device (last visited March 30, 2018).

offense—not the software installed on the devices. *United States v. Szymuszkiewicz*, 622 F.3d 701, 707 (7th Cir. 2010) (as amended Nov. 29, 2010).

And the Seventh Circuit is not the only court to conclude that software is not a device. In *Potter v. Havlicek*, 2008 WL 2556723 (S.D. Ohio 2008), a civil case alleging a violation of § 2512, the plaintiff argued that the defendant made and sold surveillance software called "Activity Monitor." The district court there found that Activity Monitor was not a device for purposes of Section 2512:

> Section 2512 makes the manufacture and/or trafficking of "any electronic, mechanical, or other device" illegal. The phrase "electronic, mechanical, or other device" is defined in 18 U.S.C. § 2510(5) to generally mean "any device or apparatus which can be used to intercept a wire, oral, or electronic communication . . . ." Clearly, Activity Monitor alone cannot be used to intercept communications. *It must be installed in a device, such as a computer, to be able to do so.*

Id. at *8 (emphasis added).

Count Five fails for a similar reason. There, the indictment alleges that Mr. Hutchins violated 18 U.S.C. § 2511 by endeavoring and procuring another person to "intercept certain electronic communications, namely computer keystrokes[.]" The Wiretap Act defines "intercept" to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any *electronic, mechanical, or other device*." 18 U.S.C. § 2510(4) (emphasis added). There can be no interception within the meaning of the statute if there is no

"electronic, mechanical, or other device." And, as explained above, Kronos is not.

For these reasons, Counts Two through Five must be dismissed for their failure to state an offense.

3. Counts One, Five, and Six Do Not Allege the Requisite Intent and Causation to Make Out Viable Claims

Counts One, Five and Six should be dismissed for an additional reason: the indictment does not allege the necessary intent and causation to state those offenses. The indictment conflates the *selling* of Kronos with *specific intent* for the buyer to commit an illegal act with Kronos.

For the conspiracy charge in Count One, the government must prove beyond a reasonable doubt that (1) there was an agreement to commit an unlawful act, (2) the defendants were parties to the agreement, and (3) one of the co-conspirators committed an overt act in furtherance of the agreement. *United States v. Archambault*, 62 F.3d 995, 999 (7th Cir. 1995). The allegations in the indictment fail because they do not meet the first prong of the test.

The conspiracy alleged in Count One is charged as one to violate 18 U.S.C. § 1030(a)(5)(A). As such, the government must establish that the defendants agreed to intentionally damage a computer. In other words, the conspiratorial objective must have been to impair the availability or integrity of data, a program, a system, or information.

But Count One's allegations do not support that conclusion. There is no claim that Mr. Hutchins or his co-defendant intended any specific result to occur because of the sale. There is no indication that they intended for the buyer to do anything in particular with the program. They did not have the requisite purpose to intentionally impair the availability or integrity of data, a program, a system, or information to support the conspiracy count.

As the Seventh Circuit has made clear in the context of drug-distribution cases, a buyer-seller relationship—without more—does not establish a conspiracy. *United States v. Johnson*, 592 F.3d 749, 759 (7th Cir. 2010). There must be an agreement "to commit a crime *other than* the crime that consists of the sale itself." *Id.* (emphasis in original) (citations omitted). To form a conspiracy, the seller must not only know that the buyer will re-sell the drugs—the buyer must *intend* for it to happen. *7th Cir. Criminal Pattern Jury Instruction* 5.10 (2012 ed.).

Likewise, conspiracy is not established here by the mere allegation that the defendants sold Kornos to a buyer—even if they knew the buyer would use it to cause damage to a computer. The indictment must also establish that Mr. Hutchins and his co-defendant specifically *intended* for the buyer to cause such damage. For Mr. Hutchins to be guilty of the charged conspiracy, his and his co-defendant's goal—their conspiratorial objective—must have been to intentionally cause the impairment of the availability or integrity of information. But this is not alleged in the indictment.

Count Six has a similar fatal flaw. This count charges Mr. Hutchins and his co-defendant with attempting to violate § 1030(a)(5)(A) by selling the program to the buyer. To establish attempt, the government must prove beyond a reasonable doubt that the defendants (1) specifically intended a completed violation of the substantive offense, and (2) took a substantial step toward completion. *United States v. Barnes*, 230 F.3d 311, 314 (7th Cir. 2000). But Count Six merely alleges an intent to give the software to a paying customer. The customer would then have to intentionally use the software to cause damage to a computer to commit the substantive offense. Selling a copy of software is not the same as using software directly to intentionally damage a computer.

Count Five has comparable failings. This count charges the defendants with knowingly and intentionally endeavoring and procuring another person to intercept electronic communications in violation of § 2511. The defendants must have taken a substantial step toward intercepting one's communications or aided and abetted someone who actually did intercept one's communications. Merely writing the program and selling it—when the actual wiretapping is the act of the buyer and up to the buyer to perform—does not meet the standard.

For these reasons, Counts One, Five, and Six do not state offenses.

CONCLUSION

Even if the government's overarching theory of Mr. Hutchins' relationship to the Kronos software is valid and provable, that theory, as alleged in the indictment, does not establish Mr. Hutchins' commission of any of the charged offenses. Each count must be dismissed.

DATED: March 30, 2018

Respectfully submitted,

/s/ Marcia Hofmann

MARCIA HOFMANN
Zeitgeist Law PC
25 Taylor Street
San Francisco, CA 94102
Email: marcia@zeitgeist.law
Telephone: (415) 830-6664

/s/ Brian E. Klein

BRIAN E. KLEIN
Baker Marquart LLP
2029 Century Park E – Suite 1600
Los Angeles, CA 90067
Email: bklein@bakermarquart.com
Telephone: (424) 652-7800

/s/ Daniel W. Stiller

DANIEL W. STILLER
DStillerLLC
Box 511130
Milwaukee, WI 53203
Email: dan@dstillerllc.com
Telephone: (414) 207-3190

Attorneys for Marcus Hutchins